



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/023,043

12/17/2001

David E. McDysan

RIC01059

5663

25537

7590

02/06/2006

MCI, INC

1133 19TH STREET NW

4TH FLOOR

WASHINGTON, DC 20036

EXAMINER

GYORFI, THOMAS A

ART UNIT

PAPER NUMBER

2135

DATE MAILED: 02/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/023,043

Applicant(s)

MCDYSAN, DAVID E.

Examiner

Tom Gyorfi

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 January 2006.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-21 remain for examination. The correspondence filed 1/10/06 amended claims 1, 9, 16, and 21.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/10/06 (with amended claims originally filed 12/8/05) has been entered.

Response to Arguments

3. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Except for the new limitations of the independent claims wherein all extra-VPN traffic is forwarded along the second logical connection, the substance of Applicant's arguments is identical to those presented in the amendment of 8/16/05. These arguments, pertaining to the alleged lack of boundary routers, ingress routers, egress routers, and treatment of denial-of-service attacks in the Seid reference were addressed

in the Final Office Action of 10/7/05. Applicant has not supplied any traversal that accounts for the evidence and analysis presented by the Examiner at that time, but has merely restated Applicant's original objections verbatim in the current amendment.

With respect to the new limitation, Examiner has determined under further consideration that Seid also discloses this limitation. Note that routers distinguish extra-VPN traffic as possessing an evpi (egress Virtual Path identifier) value of "dvpi" (col. 8, lines 30-40). Thus, standard extra-VPN traffic will always be forwarded on a different virtual path [i.e. logical connection] from any traffic belonging to a VPN (see also col. 8, lines 51-57; col. 9, lines 19-22, and Figure 7, the path represented by elements 25 and 39 in contrast to the path represented by elements 742 and 509).

Claim Rejections - 35 USC § 102

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
5. Claims 1-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Seid et al. (U.S. Patent 5,768,271).

Referring to Claim 1:

Seid discloses a network system that resists denial of service attacks on an access link to a destination host belonging to a virtual private network (VPN), said network system comprising:

one or more egress boundary routers having connections to an access network including the access link (Figs. 1-3), wherein said one or more egress boundary routers transmit intra-VPN traffic from sources within the VPN within a first access network connection (e.g. elements 742-509 of Fig. 7) and all extra-VPN traffic toward the destination host from sources outside the VPN within a second access network logical connections for extra-VPN traffic, separate from the first access network connection (Figure 7, particularly elements 25-39; and col. 4, lines 1-10); and

a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN are prevented (col. 2, line 56 – col. 3, line 15).

Referring to Claim 9:

Seid discloses a network system, comprising: an access network having an access link to a destination host belonging to a virtual private network (VPN), wherein said access network supports a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (Figure 7, and col. 4, lines 1-10); one or more egress boundary routers having connections to the access network, wherein said one or more egress boundary routers transmit intra-VPN traffic toward the destination host via the first logical connection and transmit all extra-VPN traffic toward the destination host via the second

Art Unit: 2135

logical connection (Fig. 3; col. 8, lines 13-57); a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (Ibid, and also col. 7, line 62 – col. 8, line 13), such that denial of service attacks on said access link originating from sources outside the VPN are prevented (col. 3, lines 10-15).

Referring to Claim 16:

Seid discloses a method of protecting an access link to a destination host belonging to a virtual private network (VPN) against denial of service attacks, said method comprising: in an access network including the access link, providing a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (Figure 7, and col. 4, lines 1-10); communicating, from a plurality of ingress boundary routers to one or more egress boundary routers, intra-VPN and extra-VPN traffic destined for said destination host, wherein said intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (col. 7, line 62 – col. 8, line 15); transmitting intra-VPN traffic from said one or more egress boundary routers toward the destination host via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress boundary routers toward the destination host via the second logical connection (col. 2, line 56 – col. 3, line 15), such that denial of service attacks on said access link originating from sources outside the VPN are prevented (col. 3, lines 10-15).

Art Unit: 2135

Referring to Claim 21:

Seid discloses a method for resisting denial of service attacks on an access link to a destination host included in a VPN, the method comprising the steps of: intra-VPN traffic flowing from sources included in the VPN (Figure 7, and col. 4, lines 1-10); extra-VPN traffic flowing from sources outside the VPN (Ibid); assigning a first priority level to traffic intra-VPN traffic flowing from sources included in the VPN; assigning a second priority level to traffic extra-VPN traffic flowing from sources outside the VPN; and granting, to traffic having the first priority level at the access link, precedence of access to the destination host over traffic having the second priority level (col. 10, lines 40-65; col. 12, lines 20-30), transmitting intra-VPN traffic from said one or more egress boundary routers toward the destination host via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress boundary routers toward the destination host via the second logical connection (col. 2, line 56 – col. 3, line 15).

Referring to Claims 2, 10, and 17:

Seid discloses the limitations of Claims 1, 9 and 16 above. Seid further discloses a Differentiated Services network coupling at least one of the plurality of ingress boundary routers and at least one of the one or more egress boundary routers (Figs. 1-3; observe that there exists a node that is contained within multiple VPNs and must therefore necessarily have the means to differentiate traffic in accordance with the VP-CIRs as described in col. 5, line 62 – col. 6, line 13).

Art Unit: 2135

Referring to Claims 3 and 11:

Seid discloses the limitations of Claims 1 and 9 above. Seid further discloses a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress boundary routers (col. 5, lines 40-60).

Referring to Claim 4:

Seid discloses the limitations of Claim 1 above. Seid further discloses further comprising the access network (Figs. 1-3).

Referring to Claims 5 and 12:

Seid discloses the limitations of Claims 4 and 9 above. Seid further discloses a customer premises equipment (CPE) edge router to the access link (col. 5, lines 40-60).

Referring to Claims 6, 13, and 18:

Seid discloses the limitations of Claims 5, 12 and 16 above. Seid further discloses said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic (Figure 4).

Referring to Claims 7, 14, and 19:

Seid discloses the limitations of Claims 1, 9 and 16 above. Seid further discloses at least one of said plurality of ingress boundary routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic (column 12, lines 20-30).

Referring to Claims 8, 15, and 20:

Seid discloses the limitations of Claims 1, 9 and 16 above. Seid further discloses said one or more egress boundary routers provide a plurality of different qualities of services to said intra-VPN traffic (col. 5, line 62 – col. 6, line 4).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant Admitted Prior Art (hereinafter, "AAPA") and further in view of Seid.

Referring to Claims 1, 9, and 16:

AAPA discloses a network system comprising one or more egress boundary routers having connections to an access network including the access link, wherein said one or more boundary routers transmit intra-VPN traffic and extra-VPN traffic toward the

destination host (page 3, line 13 – page 5, line 20; Figures 1 and 2), and a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol (Ibid).

AAPA does not disclose wherein intra-VPN and extra-VPN traffic are separated into a first and second logical connection, nor that the logical connections are partitioned such that denial of service attacks on said access link originating from sources outside the VPN are prevented. However, Seid discloses a method for resisting denial of service attacks (i.e. network congestion, as taught by AAPA, page 5, lines 5-10) on any packet-switched network (col. 19, lines 48-57), comprising partitioning intra-VPN traffic and all extra-VPN traffic into a first and second logical connection (Figure 7, and col. 4, lines 1-10) in such a manner as to prevent denial of service attacks on said access link originating from sources outside the VPN (col. 2, line 56 – col. 3, line 15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to partition traffic between intra-VPN and extra-VPN sources as disclosed by Seid into the network disclosed by AAPA. The motivation for doing so would be to allow a network to provide and maintain a level of service to a VPN that is unperturbed by other traffic on the network, in a manner superior to that offered by the prior art (Seid: col. 2, lines 43-46; AAPA: page 5, lines 14-20).

Referring to Claims 2, 10, and 17:

AAPA and Seid disclose the limitations of Claims 1, 9 and 16 above. Seid further discloses a Differentiated Services network coupling at least one of the plurality of

Art Unit: 2135

ingress boundary routers and at least one of the one or more egress boundary routers (Figs. 1-3; observe that there exists a node that is contained within multiple VPNs and must therefore necessarily have the means to differentiate traffic in accordance with the VP-CIRs as described in col. 5, line 62 – col. 6, line 13).

Referring to Claims 3 and 11:

AAPA and Seid disclose the limitations of Claims 1 and 9 above. Seid further discloses a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress boundary routers (col. 5, lines 40-60).

Referring to Claim 4:

AAPA and Seid disclose the limitations of Claim 1 above. Seid further discloses further comprising the access network (Figs. 1-3).

Referring to Claims 5 and 12:

AAPA and Seid disclose the limitations of Claims 4 and 9 above. Seid further discloses a customer premises equipment (CPE) edge router to the access link (col. 5, lines 40-60).

Referring to Claims 6, 13, and 18:

AAPA and Seid disclose the limitations of Claims 5, 12 and 16 above. Seid further discloses said CPE edge router having a physical port coupled to said access

link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic (Figure 4).

Referring to Claims 7, 14, and 19:

AAPA and Seid disclose the limitations of Claims 1, 9 and 16 above. Seid further discloses at least one of said plurality of ingress boundary routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic (column 12, lines 20-30).

Referring to Claims 8, 15, and 20:

AAPA and Seid disclose the limitations of Claims 1, 9 and 16 above. Seid further discloses said one or more egress boundary routers provide a plurality of different qualities of services to said intra-VPN traffic (col. 5, line 62 – col. 6, line 4).

Referring to Claim 21:

AAPA discloses a known prior art method for managing quality of service on an access link to a destination host included in a VPN, comprising assigning a first priority level to intra-VPN traffic flowing from sources included in the VPN (page 3, lines 1-11; page 4, line 14 – page 5, line 10); assigning a second priority level to extra-VPN traffic flowing from sources outside the VPN (Ibid), and transmitting intra-VPN and extra-VPN traffic from one or more egress boundary routers to the destination host (page 3, lines 13-22; Figure 1).

It is unclear from AAPA whether the traffic having the first priority level at the access link is granted precedence of access to the destination host over traffic having the second priority level, nor that the intra-VPN and extra-VPN traffic are transmitted over a first and second logical connections, respectively. However, Seid discloses the limitations regarding the priority levels (col. 10, lines 40-65; col. 12, lines 20-30) and the first and second logical connections (col. 2, line 56 – col. 3, line 15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to partition intra-VPN and all extra-VPN traffic in the manner disclosed by Seid into the network disclosed by AAPA. The motivation for doing so would be to better prevent denial of service attacks from affecting intra-VPN traffic (col. 3, lines 10-15).

Conclusion


8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: "RFC 2475: An Architecture for Differentiated Services" by S. Blake et al. Published December 1998. <http://www.ietf.org/rfc/rfc2475.txt>

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
1/27/05



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100